Remarks:

Status of the Claims

In the office action of September 15, 2009, Claims 1, 2, 4-6, 8 and 9 stand rejected.

Claims 1, 2, 5, 6 and 8 are amended herein. Claims 1-2 and 4-6, 8 and 9 are now pending in the application.

The Claims

35 USC 101

Claims 1, 2, and 4-6 were rejected under 35 USC 101 as being directed to unpatentable subject matter. Applicants have amended the claims to more particularly point out the subject matter of the invention, in particular, to more particularly tie the claims to a particular machine. Furthermore, Applicants wish to stress that a machine performing these steps has transformed itself from a machine vulnerable to differential fault analysis attack to one that is less vulnerable to such attacks. Thus, performing the method recited does cause a transformation of a material, namely the machine itself, from one state (vulnerable) to another state (less vulnerable). A differential fault analysis attack may be performed by introducing faults (e.g., to high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or even ionizing radiation to influence the operation of the processor (*Differential Fault Analysis, Wikipedia.org,* http://en.wikipedia.org/wiki/Differential_fault_analysis, accessed and printed on March 14, 2010, appended hereto as Appendix A) into the processing in the form of physical manipulation. Thus, in one aspect the states *vulnerable* and *less vulnerable* suggested here are different physical states of the machine. And accordingly, the claimed method transforms the electronic assembly from one physical state to another. Applicants posit that the claims meet the requirements of 35 USC 101 and, accordingly, request withdrawal of the rejection.

35 USC 103

Claims 1,2, 4-6, 8 and 9 stand rejected under 35 USC 103(a) as being unpatentable over Lim (U.S. Pat. Pub. 2002/0003876 A1, "Lim") in view of Sibert (U.S. Pat. No. 6,539,092 B1, "Sibert") as evidenced by Hein, James L. "Discrete Mathematics." ("Hein").

Applicants traverse the rejection.

This rejection is largely the same as the rejection given in the Office Action of April 7, 2009. Applicants' novel and non-obvious technology comprises two parts, namely, a mapping of a cipher function f(x) to another function, a *super-function*, f' that may be performed instead of f(x) and a verification function. In the Office Action of April 7, 2009, the Examiner looked to Lim for the first of these parts and to Kocher (U.S. Pat. No. 6,539,092), for the second. In the response filed on 20 August 2009, Applicants answered these rejections by demonstrating that Lim failed to teach using a super-function as defined by Applicants and that Kocher fails to teach the verification function.

The Examiner has in the present office action repeated the arguments made in the Office Action of April 7, 2009 with respect to the first part, still relying on Lim, without responding to Applicants' arguments made in the response in that regard. Applicants maintain the same arguments here, expand on the arguments further, and respectfully request an explanation from the Examiner as to why Applicants position that Lim does not teach or suggest the substitution of a *super-function* as claimed by Applicants. Lim merely describes how the standard DES algorithm works (and adds certain clocking features to allow for avoiding duplication of S-box hardware). However, as discussed in the previous office action response and herein below, Lim does not teach or suggest substituting the standard cipher function *f* with a *super-function f'* to avoid an attacker using a differential fault analysis attack being able to deduce anything about the intermediate results of the cryptographic operations performed.

The Supreme Court recently confirmed the long standing principle that an obviousness analysis begins with factual inquiries to (A) determine the scope and content of the prior art, (B) ascertaining the differences between the claimed invention and the prior art, and (C) resolving the level of ordinary skill in the pertinent art. *KSR v. Teleflex,* 82 USPQ2d 1385, 1391 (2007), (*citing with approval, Graham v. John Deere,* 383 US 1, 148 USPQ 459, (1969)).

Furthermore, "there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR,* at 1396, *quoting* (*in re Kahn*, 441 F.3d 977, 988, 78 USQP2d 1329, (Fed. Cir. 2006).

Turning now to the first of these factual inquiries, namely, the scope and content of the prior art.

It may help understanding the relationship of Lim to the art of cryptography by first briefly discussing the DES algorithm generally. Encryption and decryption using the DES algorithm is performed by a sequence of substitutions, permutations, and XOR operations. Lim states that "The DES algorithm is a 64-bit block cipher which basically have a 64-bit block input and a 64-bit block output, 56 bits among key block of the 64 bits being used for encryption and decryption and remaining 8 bits being used for parity checking. Using the DES algorithm, an encryption apparatus receives a 64-bit plain text and a 56-bit key and outputs a 64-bit cipher text." Lim, [0003]. Lim further states that "the cipher function f includes an expansion permutation unit 110, an exclusive-OR (XOR) unit 120, an S-Box permutation unit 130, a P-Box permutation unit 140 and an XOR unit 150."

Lim's Figure 1 shows the cipher function of the typical DES algorithm. Lim, [0006]. Figure 1 illustrates the components of the cipher function including the left register L(i-1) and the right register R(i-1). These registers are used in each round of the DES algorithm to produce the input to the subsequent round. For one round, the right register goes through the cipher function. The cipher function consists of an expansion unite 110, an XOR operation 120 in which the output of the expansion unit is XORed with the key, a substitution box (S-BOX) 130, and a permutation box (P-BOX) 140. The output from the P-BOX is XORed with the contents of the left register. What is being disclosed in Figure 1 of Lim is quite simply just the standard DES algorithm cipher function.

The DES algorithm, for example, by virtue of being a standard, is known. There are no secrets about the algorithm itself. Lim, for example, describes the operation of the algorithm in conjunction with Figure 1.

Applicants address the problem of differential fault analysis attacks. In a differential fault analysis attack, an attacker introduces a fault condition of some sort and analyzes the internal state of the attacked device to deduce something about the data being processed. An element of the analysis is knowledge of the algorithm being used.

There are two parts to Applicants' novel and non-obvious solution for addressing differential fault analysis attacks, namely, mapping the cipher function to another function in a reversible manner so that the cipher function may be performed using a function other than the cipher function f, and a verification step that may be used to determine if there has been a manipulation of the functions used or the results.

For the first part, the Examiner relies on Lim. However, as noted above, Lim merely teaches the use of a standard DES algorithm. As such, the cipher function of Lim does perform permutations, substitutions, and XOR operations. However, the sequence of operations are performed as prescribed by the DES algorithm and would be as expected by anyone involved cryptography.

Turning now to comparing the prior art and the claimed invention. Let's start with a summary of the invention. Applicants provide a solution that is not vulnerable to certain types of attack through the introduction of errors - attacks known as Differential Fault Analysis or Extended Fault Analysis – which attempt to obtain information about one or more data items or operations involved in an algorithm calculation by studying the calculation procedure of the electronic assembly when one or more errors are introduced. Specification, Page 1, Lines 7 – 13. The mechanism used is that a calculation that uses a function f is modified to use a function f' which is referred to as a *super-function*. A *super-function* is defined by the relationship:

$h_2(f'(h_1(x))) = f(x)$

where x is an element of a set E, h1 is defined such that it provides a one-to-one mapping of E into a set E', h2 is defined such that it provides an onto mapping of F' in F, and for any element x in E, the above equality holds. As a result, in lieu of performing the operation f(x), the super-function f' may be performed together with ancillary mappings.

Furthermore, because a Differential Fault Analysis attack uses the introduction of errors, it is useful to perform error detection on intermediate results.

Accordingly, Applicants claim executing a super-function and performing a validation check:

"performing the calculation of f(x) by performing a modified calculation of the elementary operation f(x) using a *super-function* operation acting from and/or to a larger set wherein a super-function f'" and "performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature" (Claim 1).

For the first of these limitations the Examiner points to Lim's description of the CIPHER unit for a DES algorithm. The Examiner asserts that Lim teaches performing an elementary operation using a super-function at Fig. 1, elt 130 (because this operation has a 48-bit input and a 32-bit output) of a function f for which the Examiner relies on Fig. 1, elt CIPHER FUNCTION. Office Action, Page 4, Lines 8 – 13. This is an incorrect reading of Lim.

If we consider Lim's CIPHER FUNCTION as f(x), then all the Lim has described is how to implement f(x) in terms of sub operations peformed by particular units. Lim has not taught or suggested performing the caluclation of f(x) by performing the elementary operation f(x) using a super-function (Claim 1).

A super-function is precisely defined in the claim to be a function that satifies the equality "$h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F, wherein x is a member of E and f(x) is a member of the set F." The *super-function* is a substitution function that together with the other mapping operations provide the same result as the function. Lim does not disclose one set of functions to be a substitute for another function. Rather Lim explains how the CIPHER function is to be performed using the expansion permutation 110, the S-BOX 130, and the P-Box 140. However, Lim does not teach or suggest that any of these operations can be performed using a *super-function* of any one of the operations.

The Examiner asserts that "[Lim performs] the calculation of f(x) by performing a modified calculation of the elementary operation f(x) using a super-function f'." Office Action, Page 5, Lines 1 – 3. This statement is incorrect. The examiner argues that f' is taught as element 130, the h_1 is taught by element 110 and, h_2 is taught by element 140, wherein the element CIPHER FUNCTION is equivalent to the function f(x). However, this is an overly broad reading of Lim.

A *super-function* is defined by the applicants as a function satisfying the relationship $h_2(f'(h_1(x))) = f(x)$. In other words, performing the sequence $h_1(x)$ → R1; f'(R1) → R2; $h_2(R2)$ → y would have the same result as performing f(x) → y. Doing so, Applicants avoid calculaing f(x) and avoid the operations associated with calculating f(x), thereby avoiding vulnerability to differential fault analysis attacks.

The same cannot be said for Lim. Lim merely describes the standard operations used in performing DES cryptography without suggesting hiding the operation using a super-function. Lim calculates f(x) using standard operations for calculating f(x). Where Applicants would perform corresponding operations on f'(x), Lim performs them on f(x). Therefore, Lim fails to achieve the advantages achieved by Applicants, which is not surprising because Lim does not peform the opeations suggested and claimed by Applicants, namely, mapping the input of f(x) from the set E to E', performing the corresponding super-function f' on the result of that transformation, and mappling the output from the super-function f' from the set F' to F.

For the foregoing reasons, Claim 1 is patentable over Lim.

The Examiner turns to Sibert for teaching of the verification function. This is an incorrect reading of Sibert. Applicants claim "operating the processor of the electronic assembly according to instructions stored in the storage means to perform the calculation by the verification function <u>using the result obtained by the super function</u> in order to obtain the calculation signature." Sibert, in contrast, teaches in Figures 1A and 1B, cited by the Examiner, teaches "the sender generates the message authentication code (MAC) 16 by applying MAC function 18 to plaintext 10" (Sibert, Col. 1, Line 66 – Col. 2, Line 1, and "decryption function 20 yields a plaintext representation of the message 22, which the recipient checks for authenticity by computing a MAC 24. MAC 24 is compared to MAC 16' (i.e., the received version of MAC 16)" (Col. 2, Lines 5 – 10). Thus, Sibert teaches performing the verification by computing a MAC on the input and output of the encryption and decryption operations, respectively, rather than on an intermediate calculation as specified in Applicants claims.

Sibert like Lim fails to teach or suggest mapping input and output such that a super-function (as defined in this application) may be used as a substitute for performing an elementary operation of a calculation to be secured. Therefore, Sibert fails to make up the deficiencies of Lim.

Accordingly, Claim 1 is patentable over Lim and Sibert taken singly or in combination.

Claims 6 and 8 recite analogous limitations to the limitations argued in support of Claim 1. These claims are patentable over the combination of Lim and Sibert for, at least, the reasons given in support of Claim 1.

Claims 2, 4, 5, and 9 depend from Claim 1, inherit the limitations thereof, provide further unique and non-obvious combinations, and are patentable for the reasons given in support of Claim 1 and by virtue of such further combinations.

For the foregoing reasons, the combination of Lim and Sibert taken singly or in combination does not result in Applicants' claimed invention.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: March 15, 2010

/Pehr Jansson/
Pehr Jansson

Registration No. 35,759

The Jansson Firm
3616 Far West Blvd #117-314
Austin, TX 78731
512-372-8440
512-597-0639 (Fax)
pehr@thejanssonfirm.com